

Appln No. 09/611,809

Amdt date May 17, 2004

Reply to Office action of February 17, 2004

Amendments to the Specification:

Please amend the paragraph beginning at page 8, line 26 as follows:

The instruction set used by decode unit 30 includes instructions that reduce the time required to perform the Montgomery square and Montgomery product operations. This is accomplished with specific instructions that introduce a high degree of parallelism. More specifically, these instructions cause either multiple multiplication operations to be performed simultaneously using multiplication units 34a through 34n and/or multiplication operations to be performed simultaneously with add operations using adder 38. As a result, the number of clock cycles required to complete either the ~~Montgomery~~ Montgomery square or the ~~Montgomery~~ Montgomery product is reduced. Since the equation $M = C^d \bmod N$ is so computation intensive, particularly with C and d values being 1024 bits wide, the benefits of the reduced number of cycles per iteration reduces the overall time required to establish an SSL connection. To best illustrate the operation of these instructions, several examples are provided below.

Please amend the Abstract as follows:

Methods and apparatus for an encryption processor for performing accelerated computations to establish secure network sessions. The encryption processor includes an execution unit and a decode unit. The execution unit is configured to execute

Appln No. 09/611,809

Amdt date May 17, 2004

Reply to Office action of February 17, 2004

~~Montgomery~~ and Montgomery operations and including at least one adder and at least two multipliers. The decode unit is configured to determine if a square operation or a product operation needs to be performed and to issue the appropriate instructions so that certain multiply and/or addition operations are performed in parallel in the execution unit while performing [[the]] either the Montgomery square or Montgomery product operation.